省政务服务中心安全服务项目采购需求公示

一、项目基本信息

项目名称：省政务服务中心安全服务项目

项目编号：MCHC-DZ-ZG20252271

采购预算：6,646,572.00 元

最高限价：6,646,572.00 元

二、公示期限（不少于 2 个工作日）

时间：2025 年 8 月 1 日至 2025 年 8 月 5 日

三、其他补充事宜

采购预算确定依据：贵州省本级政府采购计划书

四、项目联系人（公示期限内，优先反馈给代理机构）

1、采购人信息

采购单位名称：贵州省人民政府办公厅

项目联系人：骆毅

联系电话：0851-86986805

2、代理机构

代理全称：明诚汇采项目管理有限公司

联系人：唐永盛、聂小菊、叶勇

联系方式：0851-86892732-702

公司名称：明诚汇采项目管理有限公司

日　　期：　　2025 年 8 月 1 日

资格要求

1.满足《中华人民共和国政府采购法》第二十二条规定的资格要求如下：

(1)法人或者其他组织的营业执照等证明文件，自然人的身份证明；(2)财务状况报告(经合法审计机构出具的2024年度财务审计报告，或银行出具的有效的资信证明)；(3)依法缴纳税收（2025年任意3个月的纳税证明）和社会保障资金（2025年任意3个月的社保缴纳证明）的相关材料，纳税零申报供应商应当按照以下任意一种方式提供相应证明文件：①税务大厅零申报报表；②网络申报完成截图。依法免税或不需要缴纳社保的供应商，应提供税务机关出具的依法免税的证明文件或社会保险基金管理部门出具的不需要缴纳社会保障资金的证明文件。新成立的供应商按实际的缴纳情况提交相关证明；(4)具备履行合同所必需的设备和专业技术能力的证明材料；(5)参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明。

根据《财政部关于在政府采购活动中查询及使用信用记录有关问题的通知》（财库〔2016〕125 号）规定，供应商的信用记录作为本项目资格审查的重要依据。信用记录查询渠道由采购代理机构通过“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）查询、记录和证据留存，查询截止时点为开标当日评审前。信用信息使用规则：由代理机构对供应商信用记录进行甄别，对列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为记录名单及其他不符合《中华人民共和国政府采购法》第二十二条规定条件的供应商，应当拒绝其参与政府采购活动。

2.落实政府采购政策需满足的资格要求：本项目A包、C包均专门面向中小企业（含监狱企业、残疾人福利性单位）采购，B包面向所有企业采购，A包、C包非中小企业投标将被拒绝；

3.本项目的特定资格要求：C包供应商须具有公安部第三研究所颁发的《网络安全等级测评与检测评估机构服务认证证书》。

商务要求

★第二节　商务要求

（商务要求均为实质性要求，不接受负偏离，负偏离视为无效投标。）

一、服务期限及服务地点

（一）服务期限：

A包、B包：1年，具体在合同中约定。

C包：合同签订后，在甲方要求启动的时间起60个日历日内，通过等保测评并获得网安部门的等保登记证书。

（二）服务地点：采购人指定地点

二、基本要求

（一）供应商须提供本项目负责人、联系电话、地址。

（二）本项目整包中标，供应商必须对此次采购的所有服务进行总体报价，不得拆分项目内容投标，否则按无效投标处理。

三、付款方式

A包：

（一）项目合同签订，且在收到乙方出具的《付款申请书》和等额正规发票后15个工作日内，甲方向乙方支付合同价款的80%；

（二）项目通过采购人组织的服务验收，且在收到乙方出具的《付款申请书》和等额正规发票后15个工作日内，由甲方向乙方支付合同价款的20%。

B包：

（一）项目合同签订，且在收到乙方出具的《付款申请书》和等额正规发票后15个工作日内，甲方向乙方支付合同价款的30%；

（二）项目通过采购人组织的中期评价，且在收到乙方出具的《付款申请书》和等额正规发票后15个工作日内，由甲方向乙方支付合同价款的40%。

（三）项目通过采购人组织的服务验收，且在收到乙方出具的《付款申请书》和等额正规发票后15个工作日内，由甲方向乙方支付合同价款的30%。

C包：

项目通过采购人组织的服务验收，且在收到乙方出具的《付款申请书》和等额正

规发票后15个工作日内，由甲方向乙方支付合同价款的100%。

注：本项目付款方式以最终签订合同为准。

四、验收标准

按照国家规定的行业标准、招标文件、响应文件、采购合同及《贵州政务服务网运维管理暂行办法》规定的内容进行验收。

五、其他要求

（一）中标供应商在履行服务项目过程中专门为采购人或根据采购人提供的有关信息、资料而产生的服务成果，其知识产权和其他权益全部归采购人所有。未经采购人事先书面许可，中标供应商不得以任何形式自行使用、擅自许可任何第三方使用或向任何第三方提出有关意见和建议。

（二）中标供应商应保证其提交的服务成果不侵犯任何第三方合法享有的知识产权和其他权益。若因上述原因引起的第三方追溯，采购人概不负责，中标供应商承担由此引起的全部责任，并赔偿因此给采购人带来的全部损失。

（三）供应商须承诺：在中标公告发布之日起3个工作日内，中标供应商向采购人提供采购文件中要求提供的相关证书或资料原件；若提供材料不全或与响应文件中提供的不一致，中标供应商将被取消中标资格并上报相关部门，并承担相应法律责任。**（须提供承诺函并加盖供应商公章）**

（四）本项目A包、B包供应商若中标，应积极与上一个服务周期的服务单位衔接好服务工作，衔接的服务工作范围包含但不限于本项目正在进行的全部内容。**（须提供承诺函并加盖供应商公章）**

（五）本项目B包供应商若中标，配备专属法律服务人员（聘有法律顾问、有公司律师、或其他取得法律资格的公司员工），以应对服务期间可能会发生的网络安全、数据安全法、个人信息保护相关法律问题，出具具有法律效力的相关文书。**（须提供承诺函并加盖供应商公章）**

（六）其他未尽事宜，待中标签约时双方再议。

六、保密要求

（一）在本合同订立前、履行中及终止后，未经合同相对方书面同意，任何一方对本合同和各方相互提供的资料、信息（包括但不限于商业秘密、技术资料、图纸、数据以及与业务有关的客户信息及其他信息等）负保密责任。

（二）一方违反上述约定导致合同相对方遭受损失或不利影响的，责任方应按本合同金额的10%向合同相对方支付违约金。

（三）在整个实施过程中，各方应加强成果数据的保密。原则上中标供应商只能将所有成果（包括过程成果、衍生成果）提供给采购人；未经采购人许可，不得擅自将任何成果以任何方式提交给第三方，尤其应该注意对涉密文件的保存。成果包括文档、图表、数据库等，无论是纸质的还是电子的。成果数据的任何格式或者任何复制品均视同原始成果数据。编制单位对成果数据不拥有复制、传播、出版、翻译成外国语言等权利，不得以商业目的使用该数据或者开发和生产产品，不得将数据或衍生成果在互联网上登载。编制单位若违反有关保密规定的，依照《中华人民共和国保密法》、《中华人民共和国测绘成果管理规定》等有关法律法规的规定处理。

（四）中标供应商对采购人提供的资料负有保密责任，委托工作完成后，中标供应商归还或及时销毁采购人提供的全部资料。

七、投标有效期

提交响应文件截止之日起90个日历日。

服务内容及要求

（服务内容及要求均为实质性要求，不接受负偏离，负偏离视为无效投标。）

A 包：云安全产品租用

序号	服务内容	运维内容和指标	数量
一、电信新节点-公有域-互联网			
1	下一代防火墙	具备传统防火墙、访问控制、流量控制、应用安全防护、网络入侵检测与防御功能；防护流量 100M	1 套
二、联通新节点-公有域（互联网）			
1	下一代防火墙	具备传统防火墙、访问控制、流量控制、应用安全防护、网络入侵检测与防御功能。防护流量 100M	26 套
2	下一代防火墙	具备传统防火墙、访问控制、流量控制、应用安全防护、网络入侵检测与防御功能。防护流量 200M	8 套
3	下一代防火墙	具备传统防火墙、访问控制、流量控制、应用安全防护、网络入侵检测与防御功能。防护流量 400M	3 套
4	堡垒机	1.通过堡垒机对运维人员的细粒度访问控制、运维过程的步步管控、全方位的操作审计，实现运维过程的“事前预防、事中控制、事后审计”，完全契合新等保 2.0 中安全管理中心和安全计算环境的相关要求； 2.授权点 500 个	1 套
5	零信任 VPN	1.零信任具备零信任访问控制台（TAC），采用了动态授权、身份认证、风险感知、国密算法等多项核心技术，提供了访问控制统一配置管理、Web 应用和 API 服务集中管理、用户认证与授权、风险响应、应用审计等功能，是联动各个零信任子系统的控制中心。终端环境感知系（TESS），通过多维度的终端感知与风险评估，并结合业务访问控制手段，能够实现对终端身份的唯一识别、风险的动态感知，能够将终端风险对业务的影响降到最低。	1 套

		2.授权点 100 个	
6	漏洞扫描	1.通过对系统进行安全脆弱性深度检测，发现可被利用漏洞，达到主动防御效果，可基线核查、WEB 扫描 2.授权点 500 个	1 套
7	数据库审计	1.以安全事件为中心，以全面审计和精确审计为基础，实时记录网络上的数据库活动，对数据库操作进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行实时告警。它通过对用户访问数据库行为的记录、分析和汇报，来帮助管理员事后生成合规报告、事故追根溯源，同时通过大数据搜索技术提供高效查询审计报告，定位事件原因，以便日后查询、分析、过滤，实现加强内外部数据库网络行为的监控与审计，提高数据资产安全。 2.授权 15 个库	1 套
8	日志审计	1.对每天所记录的信息进行审计和检查，采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于 12 个月。 2.授权资产 200 个	2 套
9	主机防病毒	1.支持可疑文件检测，支持过滤邮件病毒、文件病毒、恶意网页代码、木马后门、蠕虫等多种类型病毒查杀。 2.授权资产 250 个	250 套
10	安全管理与态势感知平台	1.具备态势感知产品能力，漏洞扫描、防病毒、防篡改、合规检查等安全能力，帮助用户实现威胁检测、响应和溯源的安全运营闭环。(网络流量分析)能够捕获全流量数据包，提供 DDoS 攻击、分片攻击、恶意挖矿、虚假源 IP 等各类异常流量检测，实现全面的网络态势分析、攻击流量溯源分析，业务性能分析、安全事件分析。	1 套

		2.授权点数 500 个,汇集安全设备的告警日志，4G	
三、信创节点			
1	下一代防火墙	具备传统防火墙、访问控制、流量控制、应用安全防护、网络入侵检测与防御功能。防护流量 100M	26 套
2	下一代防火墙	1.具备传统防火墙、访问控制、流量控制、应用安全防护、网络入侵检测与防御功能； 2.防护流量 200M	12 套
3	堡垒机	1.通过堡垒机对运维人员的细粒度访问控制、运维过程的步步管控、全方位的操作审计，实现运维过程的“事前预防、事中控制、事后审计”，完全契合新等保 2.0 中安全管理中心和安全计算环境的相关要求； 2.授权资产 500 个 3.需适配人大金仓、高斯等多种数据库的日常运维	1 套
4	零信任 VPN	1.零信任具备零信任访问控制台（TAC），采用了动态授权、身份认证、风险感知、国密算法等多项核心技术，提供了访问控制统一配置管理、Web 应用和 API 服务集中管理、用户认证与授权、风险响应、应用审计等功能,是联动各个零信任子系统的控制中心。终端环境感知系（TESS），通过多维度的终端感知与风险评估，并结合业务访问控制手段，能够实现对终端身份的唯一识别、风险的动态感知，能够将终端风险对业务的影响降到最低。 2.授权点 100 个	1 套
5	漏洞扫描	1.通过对系统进行安全脆弱性深度检测，发现可被利用漏洞，达到主动防御效果，可基线核查、WEB 扫描 2.授权资产 500 个	1 套

6	数据库审计	1.以安全事件为中心，以全面审计和精确审计为基础，实时记录网络上的数据库活动，对数据库操作进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行实时告警。它通过对用户访问数据库行为的记录、分析和汇报，来帮助管理员事后生成合规报告、事故追根溯源，同时通过大数据搜索技术提供高效查询审计报告，定位事件原因，以便日后查询、分析、过滤，实现加强内外部数据库网络行为的监控与审计，提高数据资产安全。 2.授权数据库 20 个	2 套
7	数据库审计	1.以安全事件为中心，以全面审计和精确审计为基础，实时记录网络上的数据库活动，对数据库操作进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行实时告警。它通过对用户访问数据库行为的记录、分析和汇报，来帮助管理员事后生成合规报告、事故追根溯源，同时通过大数据搜索技术提供高效查询审计报告，定位事件原因，以便日后查询、分析、过滤，实现加强内外部数据库网络行为的监控与审计，提高数据资产安全。 2.授权数据库 30 个	1 套
8	日志审计	1.对每天所记录的信息进行审计和检查，采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于 12 个月。 2.授权资产 200 个	2 套
9	主机防病毒	1.支持可疑文件检测，支持过滤邮件病毒、文件病毒、恶意网页代码、木马后门、蠕虫等多种类型病毒查杀。 2、授权资产 300 个	300 套

B包：云安全和数据安全服务

服务内容	运维内容和指标
一、云安全服务	
安全监测预警服务	1.安全监测服务。通过安排固定安全服务人员7×24小时值守，负责对贵州省政务服务中心运行维护的线上信息化平台和省级大厅本地网络的日常网络安全情况进行监测，对安全监测过程中使用到的运行工具进行维护及管理，及时对工具、策略等进行特征库更新及版本升级，并对工具的授权等信息进行管理。（人员要求：需安排至少5名专业安全服务人员进行驻场服务，保证安全服务全年度7×24小时不间断，按周和月输出52份周报、12份月报） 2.安全设备策略优化。根据用户单位信息系统的业务发展情况，对信息系统安全设备的安全策略定期进行优化，充分发挥安全设备的防护能力，保障信息系统在安全设备的防护下持续稳健运行，降低安全事件的发生几率。（输出安全设备优化月报，共计输出12份《安全设备策略优化月报》）
安全分析响应服务	1.安全分析服务。对各类安全监测设备、系统检测到的网络中的病毒、网络蠕虫、网络扫描、网络攻击、木马软件、间谍软件等各种攻击事件安全事件进行分析、恶意文件分析、脆弱性分析、全面威胁分析等内容，并及时采取相应的策略来降低安全事件带来的安全风险。 2.取证溯源服务。通过建立取证溯源机制，对发生的安全事件进行全过程分析。为取证溯源提供人员、专家、工具等，得出取证的结果，初步提供依据。 3.应急响应服务。安全专家在第一时间对省政务服务中心安全事件进行应急响应处理，使网络应用系统在最短时间内恢复正常运行，查找入侵来源，减少损失。对安全事件进行应急响应处理后，将提供详细的应急响应报告，报告中将还原入侵过程，同时给出对应的解决方案。
专项安全服务	1.安全加固、策略优化服务。通过专业的检查工具和评估方法，提供安全加固建议并对相关系统进行加固，消除信息系统上存在的已知漏洞，提升关键服务器、核心系统等重点保护对象的安全等级。同

	时，根据安全运营的实际情况和特定需求，对安全运营的监测，分析和处置等安全策略进行优化设计，使安全运营工具和服务更好地作用于安全运营工作。（共计输出 2 份《安全加固和策略优化报告》） 2.漏洞扫描。对贵州省一体化政务服务平台、贵州省“互联网+监管”平台、贵州省省级 12345 政务服务便民热线平台主机和 WEB 应用开展安全漏洞扫描，检查当前网络中是否存在高风险漏洞，给出漏洞清单和修复建议。按月开展漏洞扫描，每个平台一年 12 次，共 36 次。 3.渗透测试。对贵州省一体化政务服务平台、贵州省“互联网+监管”平台、贵州省省级 12345 政务服务便民热线平台，运用模拟黑客的攻击方法对系统和网络进行非破坏性质的攻击性测试，深层次发现系统、应用存在的安全问题，最终目标是查找系统的安全漏洞、评估系统的安全状态、提供漏洞修复建议。（1）每季度针对 3 大平台进行渗透测试，共 12 次，共出具 12 份报告。（2）安排 PTS 渗透工程师对平台进行渗透。 4.基线核查。参照工信部的安全基线标准，对贵州省一体化政务服务平台、贵州省“互联网+监管”平台、贵州省省级 12345 政务服务便民热线平台业务子系统主要从三个方面：安全漏洞、安全配置、重要状态等，建立操作系统基线、数据库基线、中间件基线、安全设备基线等。针对 3 个平台每半年分别完成 1 次服务，共计 6 次，共出具 6 份报告。 5.代码审计。对贵州省一体化政务服务平台、贵州省“互联网+监管”平台、贵州省省级 12345 政务服务便民热线平台开展代码审计工作，对程序源代码逐条进行检查和分析，发现这些源代码缺陷引发的安全漏洞，并提供代码修订措施和建议：针对 3 个平台每半年分别完成 1 次服务，共计 6 次，共出具 6 份报告。 6.重大活动保障。在数博会、国庆、两会等重大国际和国内重大活动和重要节假日等期间，提供 5*8 小时现场服务以及 7×24 小时远程服务。加强信息安全人员驻场和二线人力保障。提供值守工作方案、重保值守工作报告或总结报告。在服务期内，提供重大活动保障服务，加强现场监测相关信息系统的安全状况，现场对安全事件进行及时处理。现场人员无法处理时，需加派资深安全专家到现场进行

	保障支撑，保障在重大活动期间的网络安全可靠。 7.安全教育培训。安全问题“三分技术、七分管理”，从安全意识、安全技能（信息安全攻防演练等）、政策法规（网络安全法、等保2.0、数据安全法等解读）等方面开展培训，提升相关人员的信息安全意识、保密意识、信息安全技能等。（1）培训对象。针对贵州省政务服务中心办公人员及系统管理人员；（2）培训频次。每半年开展1次安全教育培训，共2次，单次培训时长不低于2小时。 8.网站监测服务。对贵州政务服务网进行安全监测，内容包括可用性监测、敏感词监测、木马监测、暗链监测。每月提供网站安全监测报告，并协助处理告警异常。 9.新系统/新功能上线检测。包含对贵州省一体化政务服务平台、贵州省“互联网+监管”平台、贵州省省级12345政务服务便民热线平台各业务系统功能变更、新增功能等进行安全评估，针对发现的风险问题隐患，督促相关运维厂商进行整改和反馈，复测通过后方可变更。对新系统上线从资产、设备、漏洞、基线等方面进行上线安全检查，并输出上线安全检查报告。对贵州省一体化政务服务平台、贵州省“互联网+监管”平台、贵州省省级12345政务服务便民热线平台新增上线的系统进行安全检查，包括收集系统资产信息、合规检测、接入部署安全资源、进行安全加固等工作，确保新上线的系统满足安全管理要求。
云防服务	云抗DOSS、100M业务带宽，100GDDOS防护能力、云WAF服务、WEBSHELL防护、云DNS服务、云分身服务、网站加速服务、端口隐藏服务、地域访问控制、爬虫防护、IPV6/IPV4支持、HTTP/HTTPS支持。人工专家远程咨询服务。防护时段：7X24小时。每月提供监测报告。对象：贵州省一体化政务服务平台、贵州省“互联网+监管”平台、贵州省省级12345政务服务便民热线平台。
攻防演练服务	组织第三方专业网络安全服务团队，演练模拟信息安全攻击事件，通过演练锻炼工作人员的实际处理能力；检验应急处理人员对信息安全事件、应急处理相关制度掌握情况；验证应急处置方案的有效性与可行性。加强对突发安全事件的紧急处理能力，根据可能面临的主要风险和系统特点，检验应急处理流程及突发安全事件的处理能力。开展

	2 次攻防演练服务，提供攻防演练方案及攻防演练结果报告。
网络和数据安全专家咨询服务	组织专家技术人员配合甲方，协助分析省政务服务中心网络和数据安全运行态势，解答相关咨询问题，对省级政务服务信息化系统和重点市县政务服务中心进行 3-5 次安全技术指导检查。
二、数据安全服务（提供数据安全管理体系建设服务，协助政务服务中心规范数据安全管理；提供数据资产管理服务，梳理数据资产，对数据开展分级分类，并建立管理策略，开展敏感数据与个人信息的治理，对不同数据实行有针对性的保护；提供数据风险管控服务，对数据的高频访问、指令、异常访问情况进行分析，建立通报预警与合规管理机制，实现数据场景化的安全管理；最后提供 API 接口审计管理服务，监测 API 接口中的数据访问行为、敏感信息与违法信息的监测与分析，加强数据共享交换环节的数据流转监测与接口审计，保障政务数据安全性及可靠性。）	
数据安全分析服务	通过对数据库、交互接口的日志和数据进行分析、识别潜在的安全威胁，如高频次的访问、权限滥用、未授权的访问等，快速发现并响应安全事件。
数据风险管控服务	通过对数据访问行为、指令进行监测分析，发现数据风险，并开展通报处置和合规管理。
数据安全高风险管控服务	梳理数据高风险指令，整理指令日志来源，指令的检测情况，对黑白名单进行属性管理，配置合理的指令，对存在指令、安全事件进行风险分析，形成分析报告并及时通知用户。
数据安全事件通报处置服务	对数据安全事件发生的总量、已处理和未处理的风险事件数量进行汇总梳理，分析安全事件名称、类型、安全级别、时间、源 IP、目的 IP、处理状态，对数据安全事件进行通报和处置。
数据安全符合性管理服务	分析整理数据管理合规情况，对数据文件进行合规项数量、合规数量、不合规数量、合规率的分析，包括合规项分类、合规标准、是否合规、不合规原因、处理建议等；形成数据合规管理报告。
数据安全风险评估服务	结合相关工具，对数据安全风险事件开展分析与管理，包括：1.异常账号访问检测场景；2.数据库异常信息场景；3.账号多 IP 登陆场景；4.疑似撞库攻击场景；5.疑似暴力破解场景；6.访问时长审计场景；7.用户变更检测场景；8.弱口令检测场景。
API 接口审计管理服务	针对政务服务中心接口平台全量 API 接口进行接口监测，实现 API 流量解析，风险规则定义，数据风险监测，异常行为监测。

关键接口发现管理服务	通过接口文件建立访问主体清单，并进行管理；通过接口流量识别敏感数据暴露面，避免安全管理盲区，降低数据泄露和合规风险。
数据接口合规性管理	1.通过敏感数据识别规则比对方式，监测、识别分析敏感数据未经脱敏处理直接通过明文在业务系统、Web 前台进行传输的场景； 2.通过内置违法违规关键字监测引擎，监测返回数据中是否存在的违规数据； 3.通过解析接口会话，统计会话返回数据，与预设阈值进行比对，标记返回数据量过大的日志。
追溯取证分析服务	对接口业务行为进行记录，方便企业管理人员进行查询。当发生数据安全接口事件时，支持记录访问接口/页面的日志，包括：访问源地址，访问源名称，被访页面/接口地址，被访问应用名称，目的地址，访问时间，返回数据等进行溯源取证。

C包：等级保护测评

服务内容	运维内容和指标
等级保护测评服务	
系统测评	1.对贵州省一体化在线政务服务平台、互联网+监管平台、省级12345平台、省政务服务中心本地局域网等四项内容开展一次网络安全等级保护三级测评，共包含36个子系统。 2.按照《中华人民共和国网络安全法》《信息安全等级保护管理办法》《信息安全等级保护管理办法》的要求开展等保三级备案测评服务，提交等保测评报告、等保备案证明以及项目要求的其他材料。

测评清单

序号	服务平台	服务内容	数量
1	一体化在线政务服务平台	政策兑现系统	1项
		集成套餐系统	
		网上申报系统	
		云坐席系统	
		企业之家系统	
		智慧社区	
		大厅智慧管理平台	
		数字空间	
		即时通系统	
		统一自助终端管理系统	
		电子围栏	
		人脸识别系统	
		综合受理	
		淘宝式门户	
		统一身份认证	
		事项清单	
		电子证照	
		通用审批	
		好差评系统	
		全省通办	
		接口管理平台	
		数智问政	
		可信材料	
		便民查询系统	
		表单系统	

		跨省通办系统	
		政务可视化系统	
		“贵人智办”AI助手	
2	互联网+监管平台	互联网+监管系统	1项
		贵州省"互联网+监管"（热线监管）系统	
		基于监管平台开展共性支撑和深化应用建设（舆情监管应用场景建设）	
		基于监管平台开展共性支撑和深化应用建设（信用示范园区应用场景建设）	
3	12345平台	数据汇聚中心	1项
		工单调度系统	
		话务系统	
		多媒体系统	

注：各位供应商请注意，本项目为服务类项目，项目实施过程中服务要求可能会根据实际情况进行修改或者完善，本招标文件中其他未尽事宜将在签订合同时由采购方和中标供应商在合同条款中补充完善。

评审标准

本次评标采用**综合评分法。**

综合评分法，是指投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为中标候选人的评标方法。

评分的主要因素分为价格因素、商务因素和技术因素，评分因素详见评分表，评标分值保留至两位小数。评标时，评标专家依照评分表对每个有效供应商的投标文件进行独立评审、打分。

A包：云安全产品租用

评审项	评　分　标　准		备注
报价分（10分）	投标报价得分=(评标基准价/投标报价)×10 注： 1.评标基准价指满足采购文件要求且投标价格最低的投标报价，投标报价指满足采购文件要求的各投标单位的投标报价。 2.本项目A包专门面向中小企业（含残疾人福利性单位、监狱企业）采购，供应商的投标报价不再进行价格扣除。 3.评标委员会认为供应商的报价明显低于其他通过符合性审查的供应商报价，有可能影响服务质量或者不能诚信履约的，应当要求其在合理的时间内提供书面说明，必要时提交相关证明材料；供应商不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。		**客观分**
商务分（60分）	业绩（15分）	供应商2020年1月1日至今具有类似项目业绩的，每提供1个得3分，满分15分。 注： 1.日期以合同签订之日为准； 2.类似项目指信息化系统运维服务类项目； 3.证明材料须提供合同或协议书。	**客观分**
	项目团队成员（23分）	**1.项目负责人（1人，满分6分）：** 供应商拟派本项目的项目负责人： 1.1 具有注册信息安全管理人员（CISP）证书得3分； 1.2 具有软考信息系统项目管理师证书得2分；	**客观分**

		1.3 具有网络工程师证书得1分。 **2.技术负责人（1人，满分5分）：** 供应商拟派本项目的技术负责人： 2.1 具有信息化或计算机相关专业高级及以上工程师证书得3分； 2.2 具有软考系统分析师证书得2分。 **3.数据安全负责人（1人，满分6分）：** 供应商拟派本项目的数据安全负责人： 3.1 具有注册信息安全工程师证书得3分； 3.2 具有数据安全官证书得3分。 **4.其他团队人员（不含项目负责人、技术负责人、数据安全负责人，满分6分）：** 供应商拟投入本项目的其他团队成员中，同时具有信息化或计算机相关专业中级及以上工程师证书和软考高级及以上证书每提供1人得2分，满分6分。 注： 1.同一人员不重复得分； 2.证明材料须同时提供团队人员的(1)身份证；(2)相关证书；(3)供应商为其缴纳社保证明（2025年任意3个月），提供不全对应人员不得分。	
	综合实力（22分）	供应商具有下列证书： 1.有效的质量管理体系认证证书得4分； 2.有效的信息技术服务管理体系认证证书得4分； 3.有效的信息安全管理体系认证证书得4分； 4.有效的云计算安全评估证书，得5分； 5.有效的CCRC信息安全服务资质认证（信息系统安全集成），得5分。 注： 1.上述“有效的”指(1)证书在有效期内；(2)证书未被注销或撤销。 2.证明材料提供上述证书。	**客观分**

技术分（30分）	服务方案（20分）	1.供应商根据项目需求提供**“服务方案”**，下列内容提供齐全得10分，每缺1项扣2分，扣完为止。 （1）运维服务项目概述与理解； （2）运维服务方式； （3）运维服务内容； （4）运维服务交付物； （5）运维服务团队及分工。 2.评标委员会针对**“服务方案”**进行综合评分（**主观分，请评标委员会根据分值设定进行打分）：** （1）方案科学合理、针对性、操作性强得**10分**； （2）方案基本科学合理、针对性、操作性较强得**7分**； （3）方案科学性、合理性、针对性、操作性一般得**4分**； （4）方案科学性、合理性、针对性、操作性差或方案内容缺项较多得**1分**； （5）未提供不得分。	**客观分+主观分**
	应急保障方案（10分）	1.供应商根据项目需求提供**“应急保障方案”**，下列要点提供齐全得 5 分，每缺少 1 项扣 1 分，扣完为止。 （1）应急服务流程； （2）应急实施方案； （3）应急预案； （4）重大活动及节假日期间保障方案； （5）常见故障分析。 2.评标委员会针对**“应急保障方案”**进行综合评分**（主观分，请评标委员会根据分值设定进行打分）：** （1）方案详细、具体，针对性、操作性强得 **5 分**； （2）方案完整，针对性、操作性一般得 **3 分**； （3）方案完整，针对性、操作性较差或方案内容缺	**客观分+主观分**

		项较多得1分； （4）未提供不得分。	

B包：云安全和数据安全服务

评审项	评　分　标　准		备注
报价分（10分）	投标报价得分=(评标基准价/投标报价)×10 注： 1.评标基准价指满足采购文件要求且投标价格最低的投标报价，投标报价指满足采购文件要求的各投标单位的投标报价。 2.本项目B包由小微企业（含监狱企业、残疾人福利性单位）承接，投标报价给予10%的扣除，用扣除后的价格参与评审。 3.评标委员会认为供应商的报价明显低于其他通过符合性审查的供应商报价，有可能影响服务质量或者不能诚信履约的，应当要求其在合理的时间内提供书面说明，必要时提交相关证明材料；供应商不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。		**客观分**
商务分（60分）	业绩（15分）	供应商2021年1月1日至今具有类似项目业绩的，每提供1个得3分，满分15分。 注： 1.日期以合同签订之日为准； 2.类似项目指网络安全服务类项目； 3.证明材料须提供合同或协议书。	**客观分**
	评价意见（5分）	供应商提供的上述业绩中，每附一份用户评价，且评价意见为满意、优秀或同等评价的得 1 分，满分 5 分。 注：用户评价意见须包含项目名称、业主单位名称、评价意见（满意、优秀或同等评价）、业主单位盖章，否则视为不满足。	**客观分**
	项目团队成员（20分）	**1.项目负责人（1人，满分5分）：** 供应商拟派本项目的项目负责人： 1.1 具有信息化或计算机相关专业高级及以上职称证书得2分； 1.2 具有信息系统项目管理师证书得1分；	**客观分**

		1.3 具有注册信息安全工程师证书得1分。 1.4 具有10年（含）以上网络安全服务项目实施管理经验得1分。 **2.技术负责人（1人，满分5分）：** 供应商拟派本项目的技术负责人： 2.1 具有信息化或计算机相关专业高级及以上职称证书得3分； 2.2 具有注册信息安全工程师证书得1分； 2.3 具有数据安全评估师证书得1分。 **3.数据安全负责人（1人，满分3分）：** 供应商拟派本项目的数据安全负责人： 3.1 具有数据安全评估师证书得3分。 **4.其他团队人员（不含项目负责人、技术负责人、数据安全负责人，满分7分）：** 供应商拟投入本项目的其他团队成员中，具有CISP相关技术资格证书且拥有5年以上网络安全服务项目工作经验的，每提供1人得1分，满分7分； 注： 1.同一人员不重复得分； 2.证明材料须同时提供团队人员的(1)身份证；(2)相关证书；(3)工作经验证明（如劳动合同或相关单位履职证明等）；(4)供应商为其缴纳社保证明（2025年任意3个月），提供不全对应人员不得分。	
	综合实力（20分）	供应商具有下列证书： 1.有效的质量管理体系认证证书得2分； 2.有效的信息安全管理体系认证证书得3分； 3.有效的信息安全风险评估服务资质证书得3分； 4.有效的信息安全应急处理服务资质证书得4分； 5.有效的信息系统安全运维服务资质证书得4分； 6.有效的信息系统安全集成服务证书得4分； 注：	**客观分**

		1.上述“有效的”指(1)证书在有效期内；(2)证书未被注销或撤销。 2.证明材料提供上述证书。	
技术分（30分）	服务方案（20分）	1.供应商根据项目需求提供**“服务方案”**，下列内容提供齐全得10分，每缺1项扣2分，扣完为止。 （1）运维服务项目概述与理解； （2）运维服务方式； （3）运维服务内容； （4）运维服务交付物； （5）运维服务团队及分工。 2.评标委员会针对**“服务方案”**进行综合评分（**主观分，请评标委员会根据分值设定进行打分）：** （1）方案科学合理、针对性、操作性强得**10分**； （2）方案基本科学合理、针对性、操作性较强得**7分**； （3）方案科学性、合理性、针对性、操作性一般得**4分**； （4）方案科学性、合理性、针对性、操作性差或方案内容缺项较多得**1分**； （5）未提供不得分。	**客观分+主观分**
	应急保障方案（10分）	1.供应商根据项目需求提供**“应急保障方案”**，下列要点提供齐全得 5 分，每缺少 1 项扣 1 分，扣完为止。 （1）应急服务流程； （2）应急实施方案； （3）应急预案； （4）重大活动及节假日期间保障方案； （5）常见故障分析。 2.评标委员会针对**“应急保障方案”**进行综合评分**（主观分，请评标委员会根据分值设定进行打分）：**	**客观分+主观分**

		（1）方案详细、具体，针对性、操作性强得 5 分； （2）方案完整，针对性、操作性一般得 3 分； （3）方案完整，针对性、操作性较差或方案内容缺项较多得1分； （4）未提供不得分。	

C包：等级保护测评

评审项	评　分　标　准		备注
报价分(10 分)	投标报价得分=(评标基准价/投标报价)×10 注： 1.评标基准价指满足采购文件要求且投标价格最低的投标报价，投标报价指满足采购文件要求的各投标单位的投标报价。 2.本项目 C 包专门面向中小企业（含残疾人福利性单位、监狱企业）采购，供应商的投标报价不再进行价格扣除。 3.评标委员会认为供应商的报价明显低于其他通过符合性审查的供应商报价，有可能影响服务质量或者不能诚信履约的，应当要求其在合理的时间内提供书面说明，必要时提交相关证明材料；供应商不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。		**客观分**
商务分(65 分)	业绩（10分）	供应商2022年1月1日至今具有同类项目业绩的，每提供1份业绩得2分，满分10分。 注： 1.日期以合同签订之日为准； 2.同类项目指等级保护测评服务类项目； 3.证明材料须提供合同。	**客观分**
	项目团队成员（28分）	1.项目负责人(1人，满分6分)： 1.1 具有高级等级保护测评师证书得1分； 1.2 具有信息安全工程师证书得1分； 1.3 具有CISP-CISE认证证书得1分； 1.4 具有CISSP认证证书得1分； 1.5 具有CISP-DSG认证证书得1分； 1.6 具有网络安全能力认证证书得1分。 2.其他团队成员(不含项目负责人，满分22分） 为保证测评质量，供应商拟投入的其他团队成员需具备专业的测评能力： 2.1 技术人员1（1人，满分7分）	**客观分**

		2.1.1 具有高级等级保护测评师证书得2分； 2.1.2 具有CISAW（风险管理专业级）证书得2分； 2.1.3 具有CCRC-数据安全官证书得1分； 2.1.4 具有CIIP-I认证证书得1分； 2.1.5 具有CIIP-A认证证书得1分； 2.2 技术人员2（1人，满分6分） 2.2.1 具有中级测评师证书得1分； 2.2.2 具有注册信息安全专业人员(CISP-CISE)证书得2分； 2.2.3 具有网络安全能力认证证书得1分； 2.2.4 具有CISAW（风险管理方向）证书得2分。 2.3 技术人员3(1人，满分3分) 2.3.1 具有渗透工程师(CISP-PTE)证书得2分； 2.3.2 具有中级网络工程师证书得1分。 2.4 技术人员4(1人，满分3分) 2.4.1 具有初级测评师得1分； 2.4.2 具有中级安全管理人员（CCSS-M）证书得1分； 2.4.3 具有注册信息安全专业人员(CISP-CISE)证书得1分。 2.5 应急人员(1人，满分3分) 2.5.1 具有CISP证书得1分； 2.5.2 具有CCSS-R(应急响应能力认证)证书得1分； 2.5.3 具有CNVD（国家信息安全漏洞共享平台）原创漏洞证明得1分。 注： 1.同一人员不重复得分。 2.证明材料须提供项目团队成员的(1)相关证书；(2)供应商为其缴纳社保证明（2025年任意3个月），提供不全对应人员不得分。	
	技术水平	供应商在本项目中所采用的测评工须具备安全性、	**客观分**

	（4分）	高效性，包括但不仅限于项目管理系统、测评执行系统、测评调度系统、报告编制系统等。每提供1个自研测评工具软件著作权证书得1分，满分4分。 注：证明材料提供自研测评工具软件著作权证书。	
	综合实力（23分）	供应商具有以下认证证书： 1.中国合格评定国家认可委员会颁发的《中国合格评定国家认可委员会检验机构认可证书》（CNAS）得2分； 2.省级以上（含省级）质量技术监督部门（市场监督管理局）颁发的资质认定证书（CMA）（资质证书认定附表包含等级保护测评）得2分； 3.有效的质量管理体系认证证书得2分； 4.有效的信息安全管理体系认证证书得2分； 5.有效的隐私信息管理体系认证证书（认证范围包含网络安全等级保护测评、风险评估及应急处理）得5分； 6.中国信息安全测评中心颁发的信息安全服务资质证书（风险评估类）得3分； 7.中国信息安全测评中心颁发的信息安全服务资质证书（安全工程类）得2分； 8.工业信息安全测试评估机构能力认定证书得3分。 9.中国信息安全测评中心颁发的国家信息安全漏洞库（CNNVD）技术支撑单位等级证书的得2分。 注：证明材料须提供相关证书。	**客观分**
技术分(25 分)	服务方案（25分）	1.供应商根据项目需求提供**“服务方案”**，下列要点提供齐全得 10 分，每缺少 1 项扣 1 分，扣完为止。 （1）测评流程； （2）项目实施计划； （3）测评时间进度与人员安排； （4）技术措施方案以及质量保证措施方案；	**客观分+主观分**

		（5）工具介绍； （6）应急保障方案； （7）安全技术测评方案； （8）安全管理测评方案； （9）保密管理制度； （10）培训方案。 2.评标委员会针对以上 10 个要点进行综合评分（满分 15 分）： （1）各要点详细、具体，针对性强得 1.5 分； （2）各要点完整，针对性一般得 1.0 分； （3）各要点完整，针对性较差得0.5分。	

注：1.本项目为服务类项目，不享受政策性加分。

2.上述评分标准中要求提供的证明材料，未明确要求提供原件的，均提供扫描件并加盖公章，否则视为未提供；要求提供的证明材料，供应商须按要求提供且提供齐全，否则不得分；要求提供的证明材料，不清晰或无法识别的视为未提供。

3.上述评分中

3.1 **“第一档”**等指：

a.提供的方案基于采购需求的全口径，提出具有可行性的现状情况预判；

b.准确把握方案中的重、难点，分析各类情况可能发生的不可预见性，并尽可能列明多种详细预案；

c.针对不同的需求，能提供个性化的解决方案，可以举例论证；

d.对于资料、数据等响应方案的支持材料提供详细、具体，具有一定的论证支持性。

3.2 **“第二档”**等指：

a.方案内容对采购文件要求的条款已作完整响应；

b.只对方案作出标题式的简单论证，并未展开分析或列明可行的具体解决方案；

c.部分资料、数据等响应方案的支撑材料提供过于简单或未提供。

3.3 **“第三档”**等指：

a.方案不完整，与采购需求存在明显的响应缺项；

b.方案不切实际，操作困难，与采购需求相违背。

4.上述评分中，评审专家对“客观分”的评审须保持一致。

（三）价格分的计算：

1.价格分采用低价优先法计算，即满足采购文件要求的前提下，最低有效投标报价作为评标基准价，其价格分为最高。其余供应商价格分统一按照下列公式计算：

投标报价得分＝（评标基准价/投标报价）×报价分

2.评标过程中，不得去掉报价中的最高报价和最低报价。

3.因落实政府采购政策进行价格调整的，以调整后的价格计算评标基准价和投标报价。

（1）中小企业价格扣除（含监狱企业、残疾人福利性单位），在供应商资格、符合性审查均满足招标文件的前提下：

1）如专门面向中小企业采购，投标供应商报价不享受价格扣除优惠政策。

2）如非专门面向中小企业采购，则对小型和微型企业、监狱企业、残疾人福利性单位报价给予10%的价格扣除，用扣除后的价格参与评审。价格扣除只针对投标报价未超过财政控制值的供应商有效。残疾人福利性单位属于小型、微型企业的，不重复享受政策。

①中小企业价格扣除

根据《政府采购促进中小企业发展管理办法》（财库﹝2020ﴞ46 号）及相关规定，中小企业须提供中小企业声明函且声明函所载内容必须真实，如有虚假，将依法承担相应责任，包括取消中标资格、投标保证金不予退还等。

中小企业划分标准依照工业和信息化部、国家统计局、国家发展和改革委员会、财政部联合下发的《关于印发中小企业划型标准规定的通知》（工信部联企业《2011》300 号）执行。（中小企业划型标准附后）

②监狱企业价格扣除

根据《财政部司法部关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68 号）及相关规定，监狱企业参加政府采购活动时，应当提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。

③残疾人福利性单位价格扣除

根据《三部门联合发布关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141 号）及相关规定，符合条件的残疾人福利性单位在参加政府采购活动时，应当提供《残疾人福利性单位声明函》，并对声明的真实性负责。

（四）评标总得分计算方法：

评标总得分＝F1＋F2＋……＋Fn

F1、F2……Fn分别为各项评审因素的得分；

注：以上打分计算最终得分保留小数两位。

（五）排序原则：

采用综合评分法的，评标结果按评审后得分由高到低顺序排列。得分相同的，按投标报价由低到高顺序排列；得分且投标报价相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分排名前三名的供应商为中标候选人。

（六）中标原则：

由评标委员会对符合采购要求的服务方案及质量、投标价格、供应商实力、同类项目实施经验、团队人员投入等综合进行评分，并按最终得分由高到低向采购人推荐中标供应商。